What is Claimed:

1. A method for calculating a greatest common divisor of a first binary integer, U, and a second binary integer, V, the method comprising the steps of:

a) selecting 2M most significant bits of U as a first value U_{2M} and selecting 2M corresponding bits of V as a second value V_{2M}, dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

b) determining a value T as U minus the quantity Q times V;

c) if T is less than zero, applying a correction term to Q to obtain a corrected value Q' and assigning the new value for T as U minus the quantity Q' times V;

d) assigning V to U and T to V; and

e) repeating steps a) through e) until V equals zero, whereby the value remaining in U is the greatest common divisor of the first and second binary integers.

2. A method according to claim 1, wherein:

step c) includes the step of selecting 2M most significant non-zero bits of T to define a value T_{2M}, wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1); \text{ and}$$

step c) further includes the step of calculating Q", a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

3. A method according to claim 1, wherein the first binary integer, U, has a most significant non-zero bit at bit-position B1 and the second binary integer, V, has a most significant non-zero bit at bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method further including the steps of:

subtracting B2 from B1 to obtain a difference value D;

comparing D to a predetermined threshold value wherein steps a) through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e) performing the steps of:

determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M;

assigning a new value to U as U times X plus Y times V; and

switching the values of U and V.

4. A method according to claim 3, wherein the step of determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M, includes the step of invoking a further GCD routine.

5. A method according to claim 4, wherein 2M equals 32 and the further GCD routine is a Euclid routine having a modified termination condition.

6. A method according to claim 4, wherein 2M equals 64 and the further GCD routine is a Lehmer routine having a modified termination condition.

7. A method according to claim 1, further including a method for calculating a value V^{-1} being the inverse of V modulo U, wherein:

step a) further includes the steps of assigning a value of zero to a temporary variable U2 and assigning a value of one to a temporary variable V2; and

step d) further includes the steps of determining a value T2 as U2 minus Q times V2, assigning the value in V2 to U2 and assigning the value T2 to V2;

whereby, at step e) when V equals zero, the value of U2 is V^{-1}.

8. A method according to claim 3, further including a method for calculating a value V^{-1} being the inverse of V modulo U, wherein:

step a) further includes the steps of assigning a value of zero to a temporary variable U2 and assigning a value of one to a temporary variable V2; and

step d) further includes the steps of determining a value T2 as U2 minus Q times V2, assigning the value in V2 to U2 and assigning the value T2 to V2;

the step of assigning a new value to U as U times X plus Y times V, further includes the step of determining the value T2 as X times U2 plus Y times V2; and

the step of switching the values of U and V further includes the step of assigning the value of V2 to U2 and assigning the value T2 to V2;

whereby, at step e), when V equals zero, the value of U2 is V^{-1}.

9. A method for defining a Finite field that includes encryption keys for an encryption algorithm, comprising the steps of:

a) selecting a first binary integer value, P, having a number of bits such that the Finite field defined as values ranging between zero and the first value are sufficient for the encryption algorithm to be secure;

b) determining if P is a prime number, comprising the steps of:

calculating a greatest common divisor of P, and a second binary integer, V, wherein V is a product of predetermined prime numbers, including the steps of:

b1) assigning P to a temporary variable U;

b2) selecting 2M most significant non-zero bits of U as a first value U_{2M} and selecting 2M corresponding bits of V as a second value V_{2M}, dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

b3) determining a value T as U minus the quantity Q times V;

b4) if T is less than zero, applying a correction term to Q to obtain a corrected value Q' and assigning the new value for T as U minus the quantity Q' times V;

b5) assigning V to U and T to V; and

b6) repeating steps a) through e) until V equals zero, whereby the value remaining in U is the greatest common divisor of the first and second binary integers;

c) if U is greater than one, selecting an other value for P and repeating steps b) through c) until U is equal to one;

d) when U is equal to one after step c), passing P to a probabilistic primality testing routine to determine if P is prime;

whereby when P is prime, the integers from 0 to P define the Finite field.

10. A method according to claim 9, wherein:

step b4) includes the step of selecting 2M most significant non-zero bits of T to define a value T_{2M}, wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1);\text{ and}$$

step c) further includes the step of calculating Q", a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

11. A method according to claim 10, wherein the first binary integer, U, has a most significant non-zero bit at bit-position B1 and the second binary integer, V, has a most significant non-zero bit at bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method further including the steps of:

subtracting B2 from B1 to obtain a difference value D;

comparing D to a predetermined threshold value wherein steps a) through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e) performing the steps of:

determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M;

assigning a new value to U as U times X plus Y times V; and

switching the values of U and V; and

after step e) if U is greater than 1, further processing U to remove spurious factors.

12. A method according to claim 11, wherein the step of determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M, includes the step of invoking a further GCD routine.

13. A method according to claim 12, wherein 2M equals 32 and the further GCD routine is a Euclid routine having a modified termination condition.

14. A method according to claim 12, wherein 2M equals 64 and the further GCD routine is a Lehmer GCD routine having a modified termination condition.

15. A method for identifying an encryption value in a Finite field, F_P, where P is a prime number, based on a private key PV and a received public key PB, comprising the steps of:

determining a mathematical inverse of PB modulo P by performing the steps of:

a) assigning P to a temporary variable U and assigning PB to a temporary variable V and assigning a value of zero to a temporary variable U2 and assigning a value of one to a temporary variable V2;

b) selecting 2M most significant bits of U as a first value U_{2M} and selecting 2M most significant bits of V as a second value V_{2M}, dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

c) determining a value T as U minus the quantity Q times V;

d) if T is less than zero, applying a correction term to Q to obtain a corrected value Q' and assigning the new value for T as U minus the quantity Q' times V;

e) determining a value T2 as U2 minus Q times V2, assigning the value in V2 to U2, assigning the value T2 to U2, assigning V to U and T to V; and

f) repeating steps a) through e) until V equals zero, whereby the value remaining in U2 is the mathematical inverse of PB; and

dividing PV by PB modulo P by multiplying PV times the mathematical inverse of PB, wherein the result is the encryption value.

16. A method according to claim 15, wherein:

step d) includes the step of selecting 2M most significant bits of T to define a value T_M, wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1); \text{ and}$$

step d) further includes the step of calculating Q", a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

17. A method according to claim 15, wherein the variable U has a most significant bit at bit-position B1 and the variable V has a most significant bit at bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method further including the steps of:

subtracting B2 from B1 to obtain a difference value D;

comparing D to a predetermined threshold value wherein steps a) through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e) performing the steps of:

determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M;

assigning a new value to U as U times X plus Y times V and determining the value T2 as X times U2 plus Y times V2; and

switching the values of U and V and assigning the value of V2 to U2 and assigning the value T2 to U2.

18. A method according to claim 17, wherein the step of determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M, includes the step of invoking a further GCD routine.

19. A method according to claim 17, wherein 2M equals 32 and the further GCD routine is a Euclid routine having a modified termination condition.

20. A method according to claim 17, wherein 2M equals 64 and the further GCD routine is a Lehmer routine having a modified termination condition.